TECHNICAL ARCHITECTURE REVIEW

Project Name:	**Employee Gateway**
Requestor:	Greg Mead and Darcie Trimble
Date of Initial Request:	November 5, 2007
Request Description:	Consolidate existing approved Employee Gateway documents into a TA Review document.
Agency or Agencies:	DHRM, PMO, Solution Delivery
Reviewers:	Bob Woolley
ARB Acceptance Date:	
Agency Requestor Acceptance Date:	

Introduction

The business requirements for a portal/gateway environment for the State of Utah are driven by Department of Human Resource Management (DHRM) business requirements, which include the following:

- Provide a browser-based user interface.
- Be scalable to an enterprise and not just meet the demands of a single agency.
- Make information that is "owned" and maintained by different agencies available in a way that is quick, easy, and seamless for employees to access. The "work" of finding and processing the information should be done by the gateway and not the employee.
- Extend online functionality to allow greater employee self-service data entry and inquiry of their personal information.
- Provide enough relevant information at the employee gateway to allow an employee to answer his or her own questions about coverage, balances, job postings, etc., without needing support.
- Reduce the need to enter the same personal information in multiple places (address change, enrollment information, etc.).
- Maintain security, crossover, and statutory responsibilities of non-State organizations (PEHP, URS, MBI, Dental Select).
- Maintain existing security and administrative domains.

- Provide an authentication mechanism that maintains security levels for all involved organizations, and that is compatible with each organization's access controls.
- Accommodate existing systems requirements for processes which are batch oriented, time delayed, or in any way not conducted in real time.
- Interface with each organization's existing systems with minimal or no changes to existing infrastructure.
- Seamlessly direct employees to vendor (PEHP/URS/Altius/Liberty/ etc.) Web sites for detailed information.
- Allow for automated notifications of certain types of actions. For example, when provisioning required work tools or materials to an employee the system should notify the appropriate staff responsible to get the needed work related material.
- Provide notification of communications issuing from the State and agencies, including library and reference materials, policies and procedures, and other important information.
- Allow for single sign on capability to decrease the number of user IDs and passwords needed by the employee to access cross-agency information.
- Support up to 25,000 employee users.
- Support content contribution and management for, at a minimum, the following business functions:

    - recruitment (new hire and existing State employees);
    - employment application (new hire and existing State employees);
    - candidate selection (new hire and existing State employees);
    - enrollment, change, eligibility, and termination of benefits;
    - IT provisioning (new hire, role/job change, and de-provisioning for termination);
    - payroll; and,
    - life change update (marriage, change in dependents, etc.).

- Support the employment lifecycle and other Employee Gateway (EG) goals.

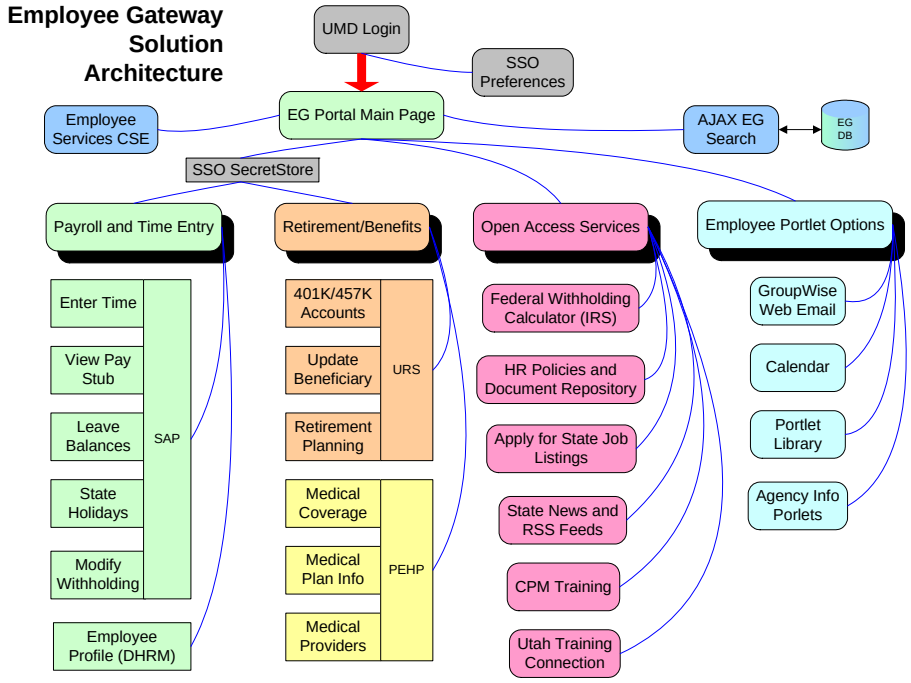
Objectives and Scope of Review

This review is principally a validation and restatement of prior documentation prepared for the EG solution that has already been approved at the CIO and agency sponsor level. The purpose of the due diligence research was to review portal solutions that could be utilized in support of an Employee Gateway for the State of Utah. The report and subsequent analysis was based on business requirements for the gateway. The report provided Employee Information Portal (EIP) research that included:

- A Summary of EIP Research
  - Commercial EIP Solutions
  - Open Source EIP Solutions
- Technical Requirements
- Architectural Implications
- Solution Analysis and Recommendations

Approved Architecture

The Employee Gateway will utilize a great deal of existing infrastructure and a few new components. The Employee Gateway solution component architecture is illustrated in the diagram that follows:



A brief listing of the key technologies includes:

Utah Master Directory: This resource has already been implemented and no new licensing is required.

Novell SecretStore: This technology is already available with the UMD and e-Directory. No new licensing is required.

Employee Gateway Portal: A portlet container application, such as JetSpeed 2, running under Apache Tomcat and Apache Web servers.

GroupWise e-Mail and Calendar Portlet: This portlet is available at no charge from Novell, but it is currently available only in a beta test release.

SSO/UMD/SecretStore Communication Module: This code must be developed for integration with the Employee Gateway and Single Sign-on (SSO) functionality. Code developed for this project will initially be limited in scope of use to the Employee Gateway and does not constitute any kind of standard.

Custom Portlets: A limited number of custom portlets must be developed (for example, an Agency Information Portlet).

Google Custom Search Engine and AJAX: The code for the AJAX function must be adapted and integrated with the Employee Gateway, but the Google CSE code has already been written.

Employee Services Data Base: The database model has already been developed, as has the application for adding services to the database.

Best Practices Review

In an often cited and quoted report[1], the Seybold Group has identified ten key requirements for an effective enterprise information portal. These include the following:

Key #1: Easy to Use
Key #2: Universal Information Access
Key #3: Dynamic Resource Access
Key #4: Extensible
Key #5: Collaborative
Key #6: Customizable
Key #7: Proactive
Key #8: Secure
Key #9: Scalable
Key #10: Manageable

These ten requirements have been reinforced since the reports original publication by most of the major portal vendor community, and as such represent important baseline criteria for portal selection. The top reasons reported[2] for portal development include:

- Enable self service for employees and managers, especially comprehensive access to payroll and benefits.

[1] *Corporate Portals: Next Generation Business Intelligence*, Seybold Group, April 1999.
[2] Brown, Matthew et al, *Companies Offer Employee Portals, Not Portal Best Practices*, Forrester Research Trends, January 12, 2007.

- Enable collaboration and information sharing. Few employee portals actually provide these services effectively.
- Business process automation which is focused on defining and improving workflows for common processes.
- Cost reduction.
- Secure remote Web access.
- Provide online training.
- Control access to content or applications.
- Governance of corporate Internet resources.
- Access to operational dashboards and metrics.

Additional best practices for best in class companies that implement successful portals include the following:[3] [4]

- Implement an enterprise data privacy, security, and data sharing policy to facilitate consistency with access to critical content and a predictable path to best-in-class status.
- Turn content and operational data into business intelligence for employees and managers. Ensure single entry of key data as much as is practicable and implement dashboards and other data views for decision makers.
- Enable opportunities for employee self service over a wide range of activities.
- Enable meaningful opportunities for collaboration between employees.
- Use the portal to facilitate business process automation with improved workflows and integrated business process management. Enable horizontal workflows like travel authorization and expense reimbursement as high priority activities.
- Provide secure Web access to portal resources.
- Measure the impact of the portal in terms of cost reduction and improved efficiency.

Emerging Technologies and Trends

Forrester suggests that the idea of "one all purpose portal is a pipe dream."[5] New waves of integration technology are gaining traction faster than portals can adapt. Some of the technologies impacting portal investment include:

- **Internet Enabled, Free Desktop Widgets and Gadgets**—Small applications that run on the desktop and directly access the Internet, such as dictionaries, search tools, weather forecasts, and news readers are widely available. Google adds new tools on a weekly basis for their free

[3] Brown, Matthew et al, *Companies Offer Employee Portals, Not Portal Best Practices*, Forrester Research Trends, January 12, 2007.
[4] Klein, Russ, *Achieving Collaboration Excellence: Content Management, Data Integration, and the Enterprise Portal*, Aberdeen Group, August 2006.
[5] *Ibid.*

portal environment. Using a company portal for these kinds of general services is probably an outdated concept.

- **Fully Programmable Rich Clients**—These clients, unlike dedicated desktop applications, can access network resources, shared team spaces, document management systems, databases, and a variety of other collaboration services. The ability to run a composite application within a rich client may render some portal services as obsolete.

- **Lightweight Application Integration**—Applications, such as Serendipity[6] with RSS integration, use of native authentication and connectors for databases and Web services, and applications such as JustSystems[7] which uses XML to tie together data from disparate systems into visual interfaces, have a large impact on the typically heavier versions of integration found in most commercial portals.

- **AJAX**—Most portal vendors now support AJAX (Asynchronous JavaScript and XML). Many vendors are doing more with Flash and AJAX based interfaces that run outside of portal environments and add substantial value to the user by providing addition options for data integration.

To some extent portals are becoming just one of many clients available to users and are not as much of the center of the desktop as may have once been envisioned.

The primary purpose of an enterprise portal seems to be one of connecting employees and other users with information they need to make informed decisions. A successful portal hinges on availability and easy access to information. Search capabilities, as well as access to relevant applications and related data integration, are key features. A wide range of both commercial and open source solutions are available.

Financial Analysis

Financial analysis in the EG business case recommended an initial startup budget for phases one and two of $100,000. This budget has been approved by DHRM.

Security Review and Analysis

SSO, for the purposes of the gateway, will be a user optional functionality that may be employed or not as a matter of preference. Since the SSO feature needs to be secure and usable across multiple authentication environments that are not controlled by the State, an e-Directory compliant password store that meets security requirements will be implemented using Novell SecretStore®. Novell

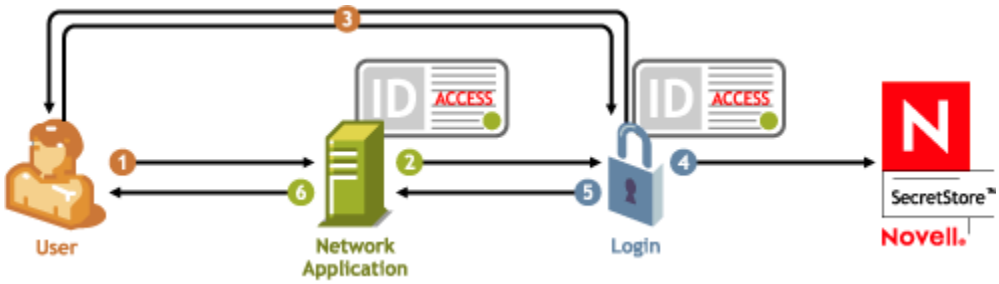
[6] *Serendipity PHP Weblog System* at http://sourceforge.net/projects/php-blog
[7] *JustSystems Software Products* at http://www.justsystems.com

SecretStore is a simple and secure password management solution. SecretStore enables users to employ a single authentication to Novell e-Directory in the form of the Utah Master Directory (UMD) to access most internally hosted Linux, Windows, and Web applications.

After UMD authentication, SecretStore-enabled applications store and retrieve the appropriate login credentials. When SecretStore is used it eliminates the need to remember or synchronize all the multiple passwords required for accessing password-protected applications and Web sites. Subsequent drawings are for illustration only; the State drawings will vary slightly to be consistent with the text descriptions. The following steps illustrate how SecretStore works:

1. A user logs in to UMD by using a password.
2. A successful login allows the user's “secrets” to be downloaded (when necessary) from SecretStore to the access gateway (EG).
3. The user accesses a Web application. The access gateway recognizes the application and responds with the appropriate user name and password from SecretStore.
4. If the access gateway does not discover matching credentials, the user is prompted to add credentials or bypass credentials stored in the UMD SecretStore.

Initial Authentication to a SecretStore-Enabled Application
The following figure illustrates the first-time authentication to an application that has been enabled for single sign-on with SecretStore.



1. Login to the EG Web site.
2. Access the protected application through the EG.
3. The gateway prompts the user to log in. The user submits credentials.
4. The gateway updates Novell SecretStore with the user's authentication information.
5. The gateway posts the users authentication information to the application or Web sites login page.
6. The user starts interacting with the application.

Subsequent Authentication to a SecretStore-enabled Application
The following figure illustrates the processes involved in subsequent user authentication to a single sign-on enabled application using SecretStore.

1. The user logs in to the EG through the UMD.
2. Access the protected application through the gateway.
3. The gateway calls Novell SecretStore to retrieve the user's authentication secrets.
4. Novell SecretStore returns the user's authentication secrets to the gateway.
5. The gateway posts the users authentication information to the application or Web site's login page.
6. The user runs a single sign-on-enabled Web application.

DTS staff will provide a Web based application that would handle the inbound and outbound communication from the SecretStore to the EG portal and would effectively eliminate any licensing exposure on the client side for SecretStore utilization. SecretStore is already provisioned with the current version of e-Directory used by the UMD.

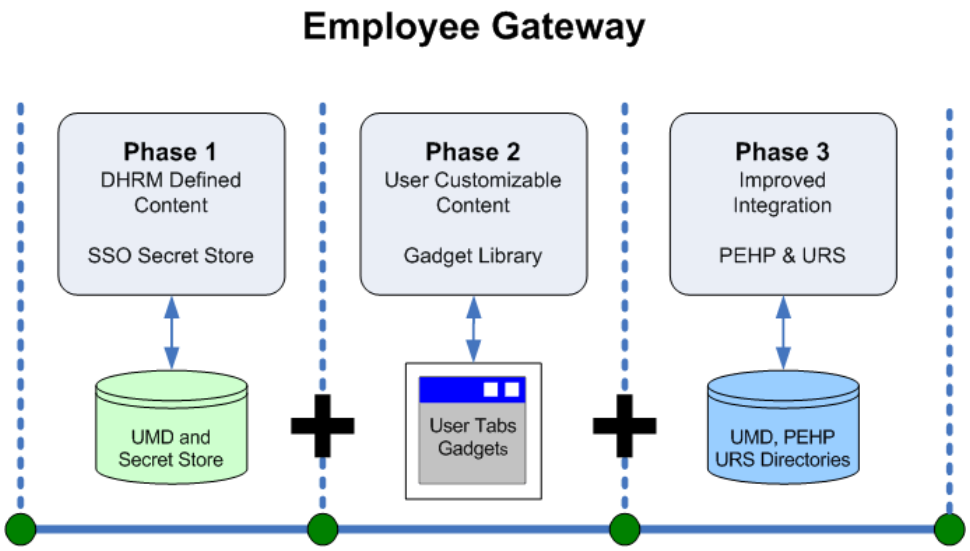
Operational and Infrastructure Analysis

The Employee Gateway uses existing infrastructure with established billing for resource utilization. No special operational issues are present.

From a development perspective after an internal technical review, no issues have been identified that pose any special concerns with JetSpeed 2. Verification of integration with external directory resources is supported, as is integration with SiteMinder. All technology stack platform components are validated.

Solution Delivery Impact and Analysis

The Employee Gateway will be designed as a Tomcat Web application that will be linked to the Utah Master Directory (UMD) for Single-Sign-On (SSO) to State Web applications such as the DHRM Employee Profile and ESS for time reporting. Gadgets/Portlets will be developed for Phase 1 and Phase 2, and a gadget/portlet library will be developed for Phase 2 using existing Google Gadget and Portlet libraries.



Deliverables

Phase 1

- Employee Gateway Web Site
- SecretStore and User Login Application
- Gadgets for Department of Human Resource Management (DHRM) Defined Content
- SiteMinder Integration

Phase 2

- Employee Gateway Web site tab functions that can be customized by the user.
- Library of gadgets/portlets approved for employee use.
- "Add More Stuff" software routine to display the gadget library and customize user tabs.

Phase 3

Improved directory integration with PEHP and URS Web sites.

The EG has been designed to provide quick wins in phases one and two. Phase one is characterized by engineering and graphic development, with only minimal coding requirements for custom portlets or gadgets. Phase two will require additional gadget/portlet development and development of a gadget/portlet library for employee use.

Agency Services Impact and Analysis

Impact on agency services is minimal. The portal will become a consumable resource for all agencies to utilize with their employees.

Summary and Recommendations

Effective employee portal implementation will place less emphasis on a quick and easily deployed portal that integrates specialized State and agency developed portlets and other Web 2.0 services from a wide variety of sources. This approach will support both commonly needed services and enable high levels of employee and agency customization as desired. In the final analysis, the best portal solution may be the one that is least expensive, standards compliant, and offers the fastest time to benefit.

References

Abrams, Charles, *Seven Ways Your Organization Can Benefit from Web 2.0*, Gartner RAS Core Research Note G00144341, November 6, 2006.

Brown, Matthew et al, *Companies Offer Employee Portals, Not Portal Best Practices*, Forrester Research Trends, January 12, 2007.

_____, *Google Search Appliance Gets Smarter*, Forrester Research Quick Take, April 19, 2006.

_____, *Single Employee Portal Vision Escapes Many Companies*, Forrester Research Trends, April 2, 2007.

_____, *Social Computing Upends Past Knowledge Management Archetypes*, Forrester Research Trends, March 8, 2007.

Corporate Portals: Next Generation Business Intelligence, Seybold Group, April 1999.

Employee Self Service Gateway Business Case (Version 5.5), Department of Human Resource Management: Salt Lake City, September, 2007.

Gootzit, David, *Magic Quadrant for Horizontal Portal Products 2006*, Gartner, Inc., May 16, 2006.

Introducing Java Portlet Specifications: JSR 168 and JSR 286 at http://developers.sun.com/portalserver/reference/techart/jsr168

JSR 286: Portlet Specification 2.0 at http://jcp.org/en/jsr/detail?id=286

Klein, Russ, *Achieving Collaboration Excellence: Content Management, Data Integration, and the Enterprise Portal*, Aberdeen Group, August 2006.

McBride, Darrus, and Doug Law, Interview regarding alternative approaches for SSO across non-State Websites, June 17, 2007.

Novell SecretStore Overview. http://www.novell.com/documentation/secretstore33/index.html?page=/documentation/secretstore33/nssadm/data/adjlgy3.html

OASIS Web Services for Remote Portlets (WSRP) at http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsrp

Open Source Portals Gaining Enterprise Adoption, Aberdeen Group Research Brief, August 2006.

Ramos, Laura, Portal Projects in Search of a Purpose, Forrester Research Trends, April 21, 2004.

State of the Portal Market 2006: Portals and the New Wisdom of the Enterprise, BEA Whitepaper, 2006.

Valdes, Ray and David Gootzit, *Portal Technologies: Fast Path to Service Oriented Architecture*, Gartner Portals, Content and Collaboration Summit, April 3-5, 2006.

Woolley, Robert D., and Dave Fletcher, *Research Report: Employee Information Portal (EIP)*, Department of Technology Services: Salt Lake City, April 19, 2007.

_____, *Employee Self Service Gateway (ESSG) Proof of Concept Technical Requirements*, Department of Technology Services: Salt Lake City, June 28, 2007.

_____, *Employee Gateway: Solution Architecture and Engineering Validation*, Department of Technology Services: Salt Lake City, August 20, 2007.